ACTA ARITHMETICA
XXXIII (1977)

Potenzreste

von

VOLKER SCHULZE (Berlin)

1. Es sei $n \in \boldsymbol{N}$ eine natürliche, $a \in \boldsymbol{Z}$ eine ganze Zahl und $P(a, n)$ die Menge aller Primzahlen p, für die die Kongruenz

$$x^n \equiv a (\mathrm{mod}\, p)$$

wenigstens eine Lösung besitzt. Die trivialen Fälle $n = 1$ oder $a = 0$ werden im folgenden ausgeschlossen. Die Primzahlmenge $P(a, n)$ wird in einer Reihe von Arbeiten untersucht (siehe Gerst [3], ferner [5]). Eine einfache Charakterisierung dieser Menge für den allgemeinen Fall ist bisher nicht bekannt. Aus den Zerlegungsgesetzen für Primideale in algebraischen Zahlkörpern ergibt sich, daß $P(a, n)$ in Spezialfällen durch Restklassen beschreibbar ist, nämlich dann, wenn der Zerfällungskörper von $x^n - a$ über $\boldsymbol{Q}$ abelsch ist; nach [5] ist dies auch nur dann möglich.

In der vorliegenden Arbeit wird untersucht, wann zwei Primzahlmengen $P(a, n)$, $P(b, m)$ übereinstimmen. Dabei werden endlich viele Ausnahmeprimzahlen nicht berücksichtigt. Wir schreiben deshalb $P(a, n) = P(b, m)$, wenn sich beide Mengen nur um endlich viele Elemente unterscheiden. Spezialfälle dieses Problems werden in verschiedenen Arbeiten behandelt. Ein erstes abschließendes Ergebnis für den Fall $n = m$ und $b = 1$ bewies Trost [6] im Jahre 1934

SATZ 1. *Es ist $P(a, n) = P(1, n)$ genau dann, wenn eine der folgenden Bedingungen erfüllt ist:*

(a) *Es gibt ein $d \in \boldsymbol{Z}$ mit $a = d^n$.*

(b) *Es ist $n \equiv 0 (\mathrm{mod}\, 8)$, und es gibt ein $d \in \boldsymbol{Z}$ mit $a = 2^{n/2} \cdot d^n$.*

Offenbar ist $P(1, n)$ die Menge aller Primzahlen. Trost gibt also ein notwendiges und hinreichendes Kriterium dafür, wann eine Kongruenz der Form $x^n \equiv a (\mathrm{mod}\, p)$ für alle Primzahlen p bis auf endlich viele Ausnahmen lösbar ist. Dieses Resultat wurde von Gerst [3] im Jahre 1970 wie folgt verallgemeinert.

SATZ 2. *Es ist $P(a,n)=P(b,n)$ genau dann, wenn es ein $t\in\mathbf{Z}$ mit $0<t<n$, $(t,n)=1$ gibt derart, daß eine der folgenden Bedingungen erfüllt ist:*

(c) *Es gibt ein $d\in\mathbf{Z}$ mit $a\cdot b^t=d^n$.*

(d) *Es ist $n\equiv 0(\mathrm{mod}\,8)$, und es gibt ein $d\in\mathbf{Z}$ mit $a\cdot b^t=2^{n/2}\cdot d^n$.*

Die Rollen von a und b können in (c) und (d) offenbar vertauscht werden. Aus beiden Ergebnissen erhält man unmittelbar

SATZ 3. *Es ist $P(a,n)=P(b,n)$ genau dann, wenn es ein $t\in\mathbf{Z}$ mit $0<t<n$, $(t,n)=1$ gibt derart, daß $P(a\cdot b^t,n)=P(1,n)$ gilt.*

Umgekehrt ergibt sich Satz 2 offenbar aus den Sätzen 1 und 3. In Abschnitt 3 wird Satz 3 direkt bewiesen. Dies liefert einen vereinfachten Beweis des Satzes 2 von Gerst. Durch eine Verallgemeinerung erhält man das Hauptergebnis dieser Arbeit, nämlich die folgende Aussage, die zusammen mit Satz 2 die eingangs gestellte Frage vollständig beantwortet.

SATZ 4. *Es sei $n=n'\cdot 2^\alpha$, n' ungerade, $m=m'\cdot 2^\beta$, m' ungerade, $\alpha\leqslant\beta$. Weiter sei $v=v(n,m)=\dfrac{n\cdot m}{(n,m)}$ das kleinste gemeinsame Vielfache von n und m, und d_3 der größte zu*

$$\frac{n\cdot m}{(n,m)^2}$$

teilerfremde Teiler von (n,m). Dann ist $P(a,n)=P(b,m)$ gleichwertig damit, daß eine der folgenden Bedingungen erfüllt ist:

(1) *Es ist $\alpha=\beta$, und es existieren Zahlen $a_1\in\mathbf{Z}$, $b_1\in\mathbf{Z}$ mit*

$$a=a_1^{n/d_3},\qquad b=b_1^{m/d_3}$$

und $P(a_1,d_3)=P(b_1,d_3)$.

(2) *Es ist $1\leqslant\alpha<\beta$, $a>0$, $b>0$, und es existieren Zahlen $a_1\in\mathbf{N}$, $b_1\in\mathbf{N}$, $t\in\mathbf{N}$, $d\in\mathbf{N}$ mit $0<t<v$, $(t,v)=1$,*

$$a^{\frac{v}{n}t}\cdot b^{\frac{v}{m}}=d^{\frac{v}{2}},\qquad a=a_1^{\frac{n}{2d_3}},\qquad b=b_1^{\frac{m}{2d_3}}.$$

Darüber hinaus muß eine der folgenden Zusatzbedingungen erfüllt sein:

(a) *Es sind a_1,b_1 Quadratzahlen.*

(b) *Es ist a_1 Quadratzahl, $\beta\geqslant 3$, $\mathbf{Q}(\sqrt{d})=\mathbf{Q}(\sqrt{2})$.*

(c) *Es ist $\alpha\geqslant 3$, $\mathbf{Q}(\sqrt{d})\subseteq\mathbf{Q}(\sqrt{a_1})=\mathbf{Q}(\sqrt{2})$.*

(3) *Es ist $\alpha=1$, $\beta=2$, $a<0$, $b<0$, $|a|$ Quadrat einer Zahl aus $\mathbf{Z}$ und $P(-2^n\cdot a^2,2n)=P(b,m)$.*

(*Nach* (1) *ist bekannt, wann diese Gleichung gilt.*)

(4) *Es ist $0=\alpha<\beta$ und $P(a^2,2n)=P(b,m)$.*

(*Nach* (1) *und* (2) *ist bekannt, wann diese Gleichung gilt.*)

Der Beweis des Satzes wird in Abschnitt 4 ausgeführt.

2. Zunächst werden einige Hilfssätze zusammengestellt. Mit $\mathbf{Q}_n$ wird der n-te Kreisteilungskörper bezeichnet. Stärker als bei Gerst werden hier Gesetze über die Zerlegung von Primidealen in algebraischen Zahlkörpern ausgenutzt. Es gilt (siehe [5])

HILFSSATZ 1. *Es ist $P(a,n)=P(b,m)$ genau dann, wenn es keinen Automorphismus des Zerfällungskörpers von $(x^n-a)(x^m-b)$ gibt, der eine Nullstelle von nur einem der beiden Polynome x^n-a, x^m-b auf sich abbildet.*

Wie Gerst [3] benötigen wir die beiden folgenden Aussagen.

HILFSSATZ 2. *Gilt $P(a,n)=P(b,n)$, so stimmen die Zerfällungskörper der Polynome x^n-a und x^n-b über $\mathbf{Q}$ überein.*

HILFSSATZ 3. *Stimmen die Zerfällungskörper von x^n-a und x^n-b über $\mathbf{Q}$ überein, so gibt es ein $t\in\mathbf{Z}$ mit $0<t<n$, $(t,n)=1$ und ein $\nu\in\mathbf{Q}_n$ mit $a\cdot b^t=\nu^n$.*

Ferner gelten die folgenden beiden Aussagen.

HILFSSATZ 4 (Schinzel [4]). *Eine Zahl $c\in\mathbf{Z}$ besitzt die Darstellung $c=\nu^n$ mit $\nu\in\mathbf{Q}_n$ genau dann, wenn eine der folgenden Bedingungen gilt:*

(a) *$n\equiv 1(\mathrm{mod}\,2)$ und es gibt ein $d\in\mathbf{Z}$ mit $c=d^n$.*

(b) *$n\equiv 0(\mathrm{mod}\,2)$ und es gibt ein $d\in\mathbf{Z}$ mit $c=d^{n/2}$, $\sqrt{d}\in\mathbf{Q}_n$.*

(c) *$n\equiv 4(\mathrm{mod}\,8)$ und es gibt ein $d\in\mathbf{Z}$ mit $c=-2^{n/2}\cdot d^{n/2}$, $\sqrt{d}\in\mathbf{Q}_n$.*

HILFSSATZ 5 (Gerst [3]). *Es sei*

$$n=2^m\cdot q_1^{a_1}\cdot\ldots\cdot q_s^{a_s}\geqslant 3$$

eine natürliche Zahl, $a_i>0$, $m\geqslant 0$, q_i paarweise verschiedene ungerade Primzahlen und $l\in\mathbf{Z}$ quadratfrei. Genau dann ist $\mathbf{Q}(\sqrt{l})$ ein quadratischer Teilkörper von $\mathbf{Q}_n$, wenn l die Darstellung

$$l=(-1)^e\cdot 2^{e_0}\prod_{i=1}^{s}(-1)^{\left(e_i\cdot\frac{q_i-1}{2}\right)}\cdot q_i^{e_i}$$

besitzt, wobei

$$e=e_0=0,\quad \text{falls}\quad m=0,1,$$
$$e_0=0,\quad \text{falls}\quad m=2,$$

und anderenfalls e,e_0,e_i unabhängig voneinander die Werte 0 oder 1 annehmen können, außer $e=e_0=e_i=0$ für alle i.

Unmittelbar einzusehen ist

HILFSSATZ 6. *Ist $q>3$ eine Primzahl, so gibt es einen von der Identität verschiedenen Automorphismus von $\mathbf{Q}_q(i)$, der i und $\sqrt{q}$ auf sich abbildet.*

Mit der Bezeichnung $\xi_n = e^{2\pi i/n}$ gilt

HILFSSATZ 7. *Ein Automorphismus α von $\boldsymbol{Q}_n$ mit $\alpha(\xi_n) = \xi_n^{1+j}$ läßt den Teilkörper $\boldsymbol{Q}_m$ genau dann invariant, wenn $m \mid j$.*

Beweis. Zu $m \mid j$ ist

$$\alpha(\xi_n^{\frac{n}{m}}) = \xi_n^{\frac{n}{m}+j\frac{n}{m}} = \xi_n^{\frac{n}{m}}$$

gleichwertig, und diese Gleichung gilt genau dann, wenn $\boldsymbol{Q}_m$ invariant bleibt.

HILFSSATZ 8. *Es sei α ein Automorphismus des Zerfällungskörpers von $x^n - a$, $\sqrt[n]{a}$ eine beliebige Nullstelle des Polynoms und*

$$\alpha(\xi_n) = \xi_n^{1+j}, \qquad \alpha(\sqrt[n]{a}) = \xi_n^k \cdot \sqrt[n]{a}.$$

Genau dann läßt α eine Nullstelle von $x^n - a$ fest, wenn $(j, n) \mid k$ gilt.

Beweis. Es gibt eine Nullstelle $\xi_n^l \cdot \sqrt[n]{a}$ von $x^n - a$ mit

$$\alpha(\xi_n^l \cdot \sqrt[n]{a}) = \xi_n^{l+lj} \cdot \xi_n^k \sqrt[n]{a} = \xi_n^l \cdot \sqrt[n]{a}$$

genau dann, wenn es ein l gibt mit $l \cdot j + k \equiv 0 (\mathrm{mod}\, n)$. Hieraus ergibt sich die Behauptung.

Ein notwendiges Kriterium für $P(a, n) = P(b, m)$ ist nach [5]

HILFSSATZ 9. *Es sei $n > 1$, $m > 1$, $a \cdot b \neq 0$ und $v = v(n, m) = \dfrac{n \cdot m}{(n, m)}$. Dann ist $P(a, n) = P(b, m)$ nur möglich, wenn es ganze Zahlen t, d mit $0 < t < v$, $(t, v) = 1$ gibt derart, daß eine der folgenden Bedingungen erfüllt ist:*

(a) *Es ist $v \equiv 1 (\mathrm{mod}\, 2)$ und $a^{\frac{v}{n}} \cdot b^{-\frac{v}{m}t} = d^v$.*

(b) *Es ist $v \equiv 0 (\mathrm{mod}\, 2)$ und $a^{\frac{v}{n}} \cdot b^{-\frac{v}{m}t} = \pm d^{\frac{v}{2}}$, $\sqrt{d} \in \boldsymbol{Q}_v$.*

(c) *Es ist $v \equiv 4 (\mathrm{mod}\, 8)$ und $a^{\frac{v}{n}} \cdot b^{-\frac{v}{m}t} = -2^{\frac{v}{2}} \cdot d^{\frac{v}{2}}$, $\sqrt{d} \in \boldsymbol{Q}_v$.*

HILFSSATZ 10. *Es seien K_1, K_2 die Zerfällungskörper von $x^n - a$, $x^m - b$ über $\boldsymbol{Q}$ und $P(a, n) = P(b, m)$. Dann unterscheiden sich die Körpergrade $[K_1 : \boldsymbol{Q}_n]$ und $[K_2 : \boldsymbol{Q}_m]$ höchstens um den Faktor 2.*

Beweis. Wenn $P(a, n) = P(b, m)$ ist, muß nach Hilfssatz 1 jeder Automorphismus von K_2, der $K_1 \cap K_2$ invariant läßt, eine Nullstelle von $x^m - b$ auf sich abbilden. Ein Automorphismus von K_2, der eine Nullstelle von $x^m - b$ und $\boldsymbol{Q}_m$ invariant läßt, muß die Identität sein. Die Identität ist also der einzige Automorphismus von K_2, der $K_1 \cap K_2$ und $\boldsymbol{Q}_m$ elementweise unbewegt läßt. Deshalb spannen $K_1 \cap K_2$ und $\boldsymbol{Q}_m$ den Körper K_2 auf, und entsprechend $K_1 \cap K_2$ und $\boldsymbol{Q}_n$ den Körper K_1. Hieraus folgt

$$[K_1 : \boldsymbol{Q}_n] = [(K_1 \cap K_2) : (K_1 \cap K_2 \cap \boldsymbol{Q}_n)] = [(K_1 \cap K_2) : (K_2 \cap \boldsymbol{Q}_n)],$$
$$[K_2 : \boldsymbol{Q}_m] = [(K_1 \cap K_2) : (K_1 \cap K_2 \cap \boldsymbol{Q}_m)] = [(K_1 \cap K_2) : (K_1 \cap \boldsymbol{Q}_m)].$$

Es genügt also

$$[(K_2 \cap \boldsymbol{Q}_n) : \boldsymbol{Q}_{(n,m)}] \leqslant 2,$$
$$[(K_1 \cap \boldsymbol{Q}_m) : \boldsymbol{Q}_{(n,m)}] \leqslant 2$$

nachzuweisen. Dazu muß nur gezeigt werden, daß der größte über $\boldsymbol{Q}$ abelsche Teilkörper von K_2 (bzw. K_1) über $\boldsymbol{Q}_m$ (bzw. $\boldsymbol{Q}_n$) einen Körpergrad $\leqslant 2$ besitzt.

Es sei K ein Teilkörper von K_2 vom Grad $\geqslant 3$ über $\boldsymbol{Q}_m$. Da K_2 über $\boldsymbol{Q}_m$ zyklisch ist, gilt für eine Nullstelle $\sqrt[m]{b}$ von $x^m - b$

$$K = \boldsymbol{Q}_m(\sqrt[m]{b}^{[K_2:K]}).$$

Dann gibt es einen Automorphismus α von K über $\boldsymbol{Q}$ mit

$$\alpha(\sqrt[m]{b}^{[K_2:K]}) = \xi_m^{\frac{m}{[K:\boldsymbol{Q}_m]}} \cdot \sqrt[m]{b}^{[K_2:K]},$$

der $\boldsymbol{Q}_m$ invariant läßt, und einen Automorphismus β von K über $\boldsymbol{Q}$, welcher

$$\xi_m^{\frac{m}{[K:\boldsymbol{Q}_m]}}$$

nicht auf sich abbildet. Für die hintereinandergeschalteten Automorphismen $\alpha \circ \beta$, $\beta \circ \alpha$ folgt

$$\alpha \circ \beta(\sqrt[m]{b}^{[K_2:K]}) \neq \beta \circ \alpha(\sqrt[m]{b}^{[K_2:K]})$$

und damit die Behauptung.

HILFSSATZ 11. *Es sei K ein reeller Zahlkörper, p eine Primzahl, $b \in \boldsymbol{N}$, $\sqrt[p]{b}$ reell. Ist $\sqrt[p]{b} \notin K$, so gilt*

$$[K(\sqrt[p]{b}) : K] = p.$$

Beweis. Der Fall $p = 2$ ist trivial. Es sei also p ungerade. Es genügt $K(\sqrt[p]{b}) \nsubseteq K(\xi_p)$ nachzuweisen. Da $K(\sqrt[p]{b}, \xi_p)$ als Zerfällungskörper von $x^p - b$ über $K(\xi_p)$ zyklisch ist, folgt daraus nämlich $[K(\sqrt[p]{b}, \xi_p) : K(\xi_p)] = p$ und damit die Behauptung. Wir nehmen $K(\sqrt[p]{b}) \subseteq K(\xi_p)$ an. Dann ist

$K(\sqrt[p]{b})$ über K abelsch. Die zu $\sqrt[p]{b}$ über K konjugierten Elemente liegen also sämtlich in $K(\sqrt[p]{b})$, andererseits sind sie als Nullstellen von $x^p - b$ mit Ausnahme von $\sqrt[p]{b}$ nicht reell. Es folgt also $[K(\sqrt[p]{b}):K] = 1$ im Widerspruch zu $\sqrt[p]{b} \notin K$.

3. In diesem Abschnitt wird Satz 3 bewiesen. Es seien K_f, K_g, K_h, K die Zerfällungskörper der Polynome

$$f(x) = x^n - a, \quad g(x) = x^n - b, \quad h(x) = x^n - a \cdot b^t, \quad f(x) \cdot g(x) \cdot h(x)$$

über $\boldsymbol{Q}$, $\boldsymbol{Q}_r$ der r-te Kreisteilungskörper und

$$\xi_r = e^{2\pi i/r}.$$

Wenn nicht ausdrücklich anders betont, ist für $c \in \boldsymbol{Z}$ mit $\sqrt[n]{|c|}$ stets die positive reelle n-te Wurzel gemeint.

Zunächst wird angenommen, daß es zu $n \in \boldsymbol{N}$, $a \in \boldsymbol{Z}$, $b \in \boldsymbol{Z}$ ein $t \in \boldsymbol{Z}$ mit $0 < t < n$, $(t, n) = 1$ gibt derart, daß

$$P(a \cdot b^t, n) = P(1, n)$$

gilt. Nach Hilfssatz 1 läßt also jeder Automorphismus von K_h und damit auch jeder von K eine Nullstelle von $h(x)$ fest. Es sei α ein Automorphismus von K, der eine Nullstelle von $g(x)$ festläßt, etwa

$$\xi_{2n}^k \cdot \sqrt[n]{|b|},$$

wobei k gerade ist, falls $b > 0$, sonst ungerade. Wie gerade erwähnt läßt α auch eine Nullstelle von $h(x)$ fest, etwa

$$\xi_{2n}^l \cdot \sqrt[n]{|a \cdot b^t|},$$

wobei l gerade ist, falls $a \cdot b^t > 0$, sonst ungerade. Die Zahl $l - kt$ ist also gerade, falls $a > 0$, sonst ungerade. Zusammen folgt, daß

$$\xi_{2n}^{l-kt} \cdot \sqrt[n]{|a|}$$

eine Nullstelle von $f(x)$ ist, und α diese Nullstelle auf sich abbildet. Jeder Automorphismus α von K läßt mit einer Nullstelle von $g(x)$ also auch eine Nullstelle von $f(x)$ fest. Entsprechend läßt jeder Automorphismus von K mit einer Nullstelle von $f(x)$ auch eine von $g(x)$ fest. Ist t' nämlich eine ganze Zahl mit $0 < t' < n$, $(t', n) = 1$, $t \cdot t' \equiv 1 (\mathrm{mod} n)$, so folgt aus $P(a \cdot b^t, n) = P(1, n)$ die Gleichung $P(a^{t'} \cdot b, n) = P(1, n)$, denn mit einer Nullstelle

$$\xi_{2n}^l \cdot \sqrt[n]{|a \cdot b^t|}$$

von $x^n - ab^t$ läßt ein Automorphismus auch die Nullstelle

$$\xi_{2n}^{l \cdot t'} \sqrt[n]{|a^{t'} \cdot b|}$$

von $x^n - a^{t'} \cdot b$ fest. Insgesamt ergibt dies die Behauptung $P(a, n) = P(b, n)$.

Es sei nun $P(a, n) = P(b, n)$. Nach den Hilfssätzen 2, 3 und 4 folgt $K_f = K_g$, und es existiert ein $t \in \boldsymbol{N}$, $0 < t < n$, $(t, n) = 1$ mit $ab^t = \nu^n$, $\nu \in \boldsymbol{Q}_n$, $\nu^2 \in \boldsymbol{Z}$. Gezeigt werden muß nach Hilfssatz 1, daß jeder Automorphismus von K_h eine Nullstelle von $h(x)$ festläßt. Dies ist trivial, falls $\nu \in \boldsymbol{Z}$, da $h(x)$ dann eine Nullstelle in $\boldsymbol{Z}$ besitzt. Wir dürfen uns also im folgenden auf den Fall $\nu \notin \boldsymbol{Z}$ beschränken. Ist $n \equiv 1 (\mathrm{mod} 2)$, so folgt nach Hilfssatz 4 sofort $\nu \in \boldsymbol{Z}$. Damit ist der Satz für ungerades n bereits nachgewiesen. Im folgenden werden drei Fälle unterschieden.

(a) Es sei $n = 2k$, k ungerade. Aus der Annahme $\nu \notin \boldsymbol{Z}$ wird ein Widerspruch hergeleitet. Nach den Hilfssätzen 4 und 5 ist $\nu^2 | n$, ν^2 ungerade. Weiter seien $q_1 < \ldots < q_s$ diejenigen Primteiler von ν^2, deren Quadrat nicht Teiler von ν^2 ist. Dann gibt es nach Hilfssatz 6 einen Automorphismus α von $K_f(i)$ über $\boldsymbol{Q}$ mit folgenden Eigenschaften: Ist q ein ungerader Primteiler von n, so ist α nicht die Identität auf $\boldsymbol{Q}_q$. Weiter gilt $\alpha(\sqrt{q_1}) = -\sqrt{q_1}$, $\alpha(\sqrt{q_i}) = \sqrt{q_i}$ für $i = 2, \ldots, s$ und $\alpha(i) = i$. Offenbar folgt $\alpha(\nu) = -\nu$. Da $P(a, n) = P(b, n)$ angenommen wurde, ist nach Hilfssatz 1 ein Widerspruch hergeleitet, wenn gezeigt wird, daß α eine Nullstelle von genau einem der beiden Polynome $f(x), g(x)$ festläßt. Dies wird im folgenden nachgewiesen.

Es gelte $\alpha(\xi_{2n}) = \xi_{2n}^{j+1}$, also $\alpha(\xi_n) = \xi_n^{j+1}$. Nach Hilfssatz 7 ist dann $(j, 2n) = 4$. Offenbar gibt es zwei (nicht notwendig reelle) Nullstellen $\sqrt[n]{a}, \sqrt[n]{b}$ von $f(x), g(x)$ mit

$$\sqrt[n]{a} \cdot \sqrt[n]{b^t} = \nu.$$

Gilt

$$\alpha(\sqrt[n]{a}) = \xi_n^k \cdot \sqrt[n]{a}, \quad \alpha(\sqrt[n]{b}) = \xi_n^l \cdot \sqrt[n]{b},$$

so folgt wegen $\alpha(\nu) = -\nu$

$$2k + 2lt \equiv n (\mathrm{mod} 2n).$$

Genau eine der beiden Zahlen k, l ist also gerade; d.h. es gilt genau eine der Beziehungen

$$(j, n) | l, \quad (j, n) | k.$$

Nach Hilfssatz 8 folgt die Behauptung.

(b) Es sei $n = 2^m k$, $m > 1$, k ungerade, $ab < 0$, also etwa $a < 0$, $b > 0$. Wir zeigen, daß dieser Fall nicht eintreten kann unabhängig davon, ob ν in $\boldsymbol{Z}$ liegt oder nicht. Wie in (a) gilt $\nu^2 | n$. Weiter sei α ein Automorphismus von $K_f(\xi_{2n})$ mit $\alpha(i) = -i$, $\alpha(\sqrt{2}) = \sqrt{2}$ und der Eigenschaft,

daß für jeden ungeraden Primteiler q von n der Kreisteilungskörper Q_q nicht elementweise fest bleibt, aber $\alpha(\sqrt{q}) = \sqrt{q}$ gilt. Unmittelbar folgt

$$\alpha(|\nu|) = |\nu|, \quad |\nu| = \sqrt[n]{|a| \cdot b^t}. \tag{1}$$

Dabei ist mit $\sqrt[n]{|a| \cdot b^t}$ die positive reelle Wurzel gemeint. Es gelte weiter

$$\alpha(\xi_{2n}) = \xi_{2n}^{2j+1},$$

nach Hilfssatz 7 also

$$\alpha(\xi_n) = \xi_n^{2j+1}, \quad (2j, 2n) = 2. \tag{2}$$

Werden mit $\sqrt[n]{|a|}, \sqrt[n]{b}$ die positiven reellen Wurzeln bezeichnet, und gilt

$$\alpha(\sqrt[n]{|a|}) = \xi_n^k \cdot \sqrt[n]{|a|}, \quad \alpha(\sqrt[n]{b}) = \xi_n^l \sqrt[n]{b},$$

so ergibt sich nach (1)

$$k + lt \equiv 0 \pmod{n},$$

und daraus nach (2), daß $j+k$ gerade ist genau dann, wenn l ungerade ist. Da für die Nullstellen $\xi_{2n} \cdot \sqrt[n]{|a|}, \sqrt[n]{b}$ von $f(x), g(x)$

$$\alpha(\xi_{2n} \cdot \sqrt[n]{|a|}) = \xi_n^{k+j} \cdot \xi_{2n} \cdot \sqrt[n]{|a|}, \quad \alpha(\sqrt[n]{b}) = \xi_n^l \cdot \sqrt[n]{b}$$

gilt, liefert dies zusammen mit (2) nach Hilfssatz 8, daß a eine Nullstelle von genau einem der beiden Polynome $f(x), g(x)$ festläßt. Das ist nach Hilfssatz 1 ein Widerspruch zu $P(a, n) = P(b, n)$.

(c) Es sei $n = 2^m k$, $m > 1$, k ungerade, $a \cdot b > 0$. Weiter gelte $P(a, n) = P(b, n)$. Dann gibt es nach Hilfssatz 3 ein $t \in N$ mit $0 < t < n$, $(t, n) = 1$, $a \cdot b^t = \nu^n$, $\nu \in Q_n$. Es gilt also

$$Q(\sqrt[n]{a \cdot b^t}) = Q(\nu). \tag{3}$$

Wir setzen

$$Q_{2^{m+1}}(\sqrt[2^m]{|b|}) = K'$$

und zeigen zunächst

$$Q(\nu) \subseteq K'. \tag{4}$$

Nach Hilfssatz 11 ist

$$[Q(\sqrt[n]{|b|}) : Q(\sqrt[2^m]{|b|})]$$

und damit auch $[K'(\sqrt[n]{|b|}) : K']$ ungerade. Gilt (4) nicht, so folgt daraus $Q(\nu) \not\subseteq K'(\sqrt[n]{|b|})$. Da $K'(\sqrt[n]{|b|})$ eine Nullstelle von $g(x)$ enthält, gibt es einen Automorphismus α von K_f über Q, der Q_{2^m} invariant läßt und eine

Nullstelle von $g(x)$, etwa $\sqrt[n]{b}$, nicht jedoch ν auf sich abbildet. Im folgenden wird gezeigt, daß a keine Nullstelle von $f(x)$ auf sich abbilden kann. Dies liefert nach Hilfssatz 1 einen Widerspruch zu $P(a, n) = P(b, n)$ und damit die Beziehung (4).

Für diejenige Nullstelle $\sqrt[n]{a}$ von $f(x)$, für welche

$$\sqrt[n]{a} \cdot \sqrt[n]{b^t} = \nu$$

ist, gilt

$$\alpha(\sqrt[n]{a}) = -\sqrt[n]{a} = \xi_n^{n/2} \cdot \sqrt[n]{a}.$$

Weiter gilt nach Hilfssatz 7

$$\alpha(\xi_n) = \xi_n^{1+j} \quad \text{mit} \quad 2^m | j.$$

Beides zusammen sichert nach Hilfssatz 8, daß a keine Nullstelle von $f(x)$ festlassen kann.

Der Körper $Q(\nu)$ ist nach (4) ein reeller quadratischer Teilkörper von K'. Andererseits lassen sich alle reellen quadratischen Teilkörper von K' angeben. Offenbar ist K' als Zerfällungskörper von

$$x^{2^{m+1}} - b^2$$

zyklisch über dem 2^{m+1}-ten Kreisteilungskörper. Daraus ergibt sich zusammen mit Hilfssatz 5, daß K' nur die reellen quadratischen Zahlkörper

$$Q(\sqrt[2^l]{|b|}) \text{ und, falls } m \geqslant 3,\ Q(\sqrt{2}),\ Q(\sqrt{2} \cdot \sqrt[2^l]{|b|})$$

mit geeignetem l, $1 \leqslant l \leqslant m$, enthalten kann. Ist $m \geqslant 3$ und $Q(\nu) = Q(\sqrt{2})$, so ergibt sich nach Satz 1 die Behauptung. Es gelte also

$$Q(\nu) = Q(\sqrt[2^l]{|b|}) \text{ oder, falls } m \geqslant 3,\ Q(\nu) = Q(\sqrt{2} \cdot \sqrt[2^l]{|b|}). \tag{5}$$

Nun werden zwei Fälle unterschieden. Zunächst sei $l = m$. Dann ergibt sich aus (3) die Gleichung $Q(\sqrt[n]{|a|}) = Q$ oder, falls $m \geqslant 3$, $Q(\sqrt[n]{|a|}) = Q(\sqrt{2})$ und damit, da a und b o.B.d.A. vertauscht werden können, ebenfalls die Behauptung.

Es sei nun $l < m$. Anstelle von t wählen wir dann

$$t_1 = t \pm \frac{n}{2^l}$$

und setzen

$$\nu_1^n = a \cdot b^{t_1} = \nu^n \cdot b^{\pm \frac{n}{2^l}}.$$

Das Vorzeichen wird dabei so gewählt, daß $0 < t_1 < n$. Die Wahl von t_1 ist möglich, weil t_1 ebenso wie t zu n teilerfremd ist und außerdem $Q(\nu_1) \subseteq Q_n$. Die letzte Beziehung ergibt sich, da aus (5)

$$Q(\nu_1) = Q \text{ oder, falls } m \geqslant 3, Q(\nu_1) = Q(\sqrt{2})$$

folgt. Das Letztere liefert gleichzeitig nach Satz 1 die Gleichung $P(a \cdot b^{t_1}) = P(1, n)$ und damit die Behauptung.

4. In diesem Abschnitt wird Satz 4 bewiesen. Es sei

$$v = \frac{n \cdot m}{(n, m)} = \frac{n}{(n, m)} \cdot \frac{m}{(n, m)} \cdot d_1 \cdot d_2 \cdot d_3$$

das kleinste gemeinsame Vielfache von n und m, d_1 der größte Teiler von (m, n), der nur Primteiler von $\frac{n}{(n, m)}$ enthält, d_2 der größte Teiler von (n, m), der nur Primteiler von $\frac{m}{(n, m)}$ enthält, d_3 der größte Teiler von (n, m), der teilerfremd zu $d_1 \cdot d_2$ ist. Offenbar sind d_1, d_2, d_3 paarweise teilerfremd. Im folgenden werden drei Fälle getrennt behandelt.

(a) Es sei $v \equiv 1 \pmod 2$. Dann ist zu zeigen: Es ist $P(a, n) = P(b, m)$ genau dann, wenn es Zahlen a_1, b_1 aus Z gibt mit

$$a = a_1^{n/d_3}, \quad b = b_1^{m/d_3}$$

und $P(a_1, d_3) = P(b_1, d_3)$.

Es gelte $P(a, n) = P(b, m)$. Dann wird zunächst

$$[K_f : Q_n] \mid d_3 \cdot d_2 \tag{6}$$

bewiesen. Nach Hilfssatz 9 existieren ganze Zahlen t, d mit $0 < t < v$, $(t, v) = 1$,

$$a^{\frac{v}{n}t} \cdot b^{\frac{v}{m}} = d^v. \tag{7}$$

Ein Automorphismus des Zerfällungskörpers K von $(x^n - a)(x^m - b)$ bildet die reellen Nullstellen $\sqrt[n]{a}, \sqrt[m]{b}$ von $f(x), g(x)$ trivialerweise auf Elemente der Form

$$\xi_n^{i'} \cdot \sqrt[n]{a}, \quad \xi_m^{j'} \cdot \sqrt[m]{b}$$

ab und wegen (7) auf Elemente der Form

$$\xi_{(n,m)}^{i} \cdot \sqrt[n]{a}, \quad \xi_{(n,m)}^{j} \cdot \sqrt[m]{b}.$$

Daraus ergibt sich $[K_f : Q_n] \mid (n, m)$.

Die zu $\sqrt[n]{a}$ über Q_n konjugierten Elemente haben die Form

$$\sqrt[n]{a} \cdot \xi_v^{\frac{v}{[K_f : Q_n]} \cdot \delta}, \quad \delta = 0, 1, \ldots, [K_f : Q_n] - 1$$

oder in anderer Schreibweise

$$\sqrt[n]{a} \cdot \xi_v^{\lambda \cdot \frac{n \cdot m}{(n,m)^2} \cdot \delta}, \quad \delta = 0, 1, \ldots, [K_f : Q_n] - 1. \tag{8}$$

Dabei gilt $[K_f : Q_n] = \frac{(n, m)}{\lambda}$. Die bei (8) aufgeführten Elemente sind auch die zu $\sqrt[n]{a}$ über Q konjugierten, denn es ist

$$\sqrt[n]{a}^{[K_f : Q_n]} \in Q_n,$$

nach Hilfssatz 4 ist a also $\frac{n}{[K_f : Q_n]}$-te Potenz einer Zahl aus Z.

Zum Nachweis von (6) muß $d_1 \mid \lambda$ bewiesen werden. Da

$$d_3 \cdot \frac{n \cdot m}{(n, m)^2}$$

alle Primteiler von v enthält, und deshalb v zu

$$d_3 \cdot \lambda \cdot \frac{n \cdot m}{(n, m)^2} + 1$$

teilerfremd ist, gibt es einen Automorphismus γ von K über Q mit

$$\gamma(\xi_v^{\frac{m}{(n,m)}}) = \xi_v^{d_3 \cdot \lambda \cdot \frac{n \cdot m^2}{(n,m)^3} + \frac{m}{(n,m)}}$$

und wegen (8) außerdem mit

$$\gamma(\sqrt[n]{a}) = \xi_v^{-d_3 \cdot \lambda \cdot \frac{n \cdot m^2}{(n,m)^3}} \cdot \sqrt[n]{a}. \tag{9}$$

Gilt

$$\gamma(\xi_v) = \xi_v^{c+1}, \tag{10}$$

so folgt

$$c \cdot \frac{m}{(n, m)} \equiv d_3 \cdot \lambda \cdot \frac{n \cdot m^2}{(n, m)^3} \pmod v. \tag{11}$$

Der Automorphismus γ läßt die Nullstelle $\xi_n \cdot \sqrt[n]{a}$ von $f(x)$ fest, wegen $P(a, n) = P(b, m)$ nach Hilfssatz 1 also auch eine Nullstelle von $g(x)$, etwa

$$\xi_v^{\mu \cdot \frac{n}{(n,m)}} \cdot \sqrt[m]{b}.$$

Wegen (7) und (9) gilt

$$\gamma(\sqrt[m]{b}) = \xi_v^{t\cdot d_3\cdot\lambda\cdot\frac{n\cdot m^2}{(n,m)^3}}\cdot\sqrt[m]{b}.$$

Hieraus ergibt sich zusammen mit (10)

$$c\cdot\frac{n}{(n,m)}\cdot\mu \equiv -t\cdot d_3\cdot\lambda\cdot\frac{n\cdot m^2}{(n,m)^3}\pmod v. \tag{12}$$

Die Kongruenzen (11) und (12) werden nun ausgewertet. Aus (11) folgt

$$\frac{n}{(n,m)}\cdot\lambda \mid c.$$

Falls $d_1\nmid\lambda$, ist dies ein Widerspruch zu (12), da

$$\left(c\cdot\frac{n}{(n,m)}\cdot\mu, d_1\cdot\frac{n}{(n,m)}\right) \geqq \left(-t\cdot d_3\cdot\lambda\cdot\frac{n\cdot m^2}{(n,m)^3}, d_1\cdot\frac{n}{(n,m)}\right).$$

Damit ist (6) bewiesen.

Da $f(x)$ und $g(x)$ vertauscht werden können, gilt entsprechend (6) die Beziehung $[K_g:\boldsymbol{Q}_m]\mid d_3d_1$, nach Hilfssatz 10 also $[K_f:\boldsymbol{Q}_n]\mid d_3$, $[K_g:\boldsymbol{Q}_m]\mid d_3$. Aus dieser Beziehung ergibt sich nun, daß es Zahlen a_1, b_1 aus $\boldsymbol{Z}$ gibt mit

$$a = a_1^{n/d_3}, \quad b = b_1^{m/d_3},$$

denn a ist wie bereits erwähnt $\frac{n}{[K_f:\boldsymbol{Q}_n]}$-te Potenz einer Zahl aus $\boldsymbol{Z}$. Entsprechend gilt dies für b. Weiter folgt aus (7)

$$a_1^t\cdot b_1 = d^{d_3},$$

woraus nach Satz 2 die Beziehung $P(a_1, d_3) = P(b_1, d_3)$ folgt.

Es gelte nun umgekehrt

$$a = a_1^{n/d_3}, \quad b = b_1^{m/d_3}$$

und $P(a_1, d_3) = P(b_1, d_3)$. Dann existieren nach Satz 2 ganze Zahlen t, d mit $0 < t < d_3$, $(t, d_3) = 1$ und

$$a_1^t\cdot b_1 = d^{d_3}. \tag{13}$$

Es wird gezeigt, daß ein Automorphismus des Zerfällungskörpers von $(x^n-a)(x^m-b)$, der eine Nullstelle von x^n-a, etwa

$$\xi_v^{\delta\cdot\frac{m}{(n,m)}}\cdot\sqrt[n]{a}$$

auf sich abbildet, auch eine Nullstelle von x^m-b festläßt. Da x^n-a und x^m-b vertauscht werden können, ergibt sich hieraus die Behauptung $P(a, n) = P(b, m)$ nach Hilfssatz 1. Sind die Bilder von $\sqrt[n]{a}$, ξ_v

$$\xi_v^{-\lambda\cdot d_1\cdot d_2\cdot\frac{n\cdot m}{(n,m)^2}}\cdot\sqrt[n]{a}, \qquad \xi_v^{1+c},$$

so folgt

$$c\cdot\delta\cdot\frac{m}{(n,m)} \equiv \lambda\cdot d_1\cdot d_2\cdot\frac{n\cdot m}{(n,m)^2}\pmod v.$$

Wegen (13) ist zu zeigen, daß ein $\mu\in\boldsymbol{Z}$ existiert mit

$$\mu\cdot c\cdot\frac{n}{(n,m)} \equiv -t\cdot\lambda\cdot d_1\cdot d_2\,\frac{n\cdot m}{(n,m)^2}\pmod v.$$

Da aufgrund der ersten Kongruenz (c, v) und damit auch $\left(c\cdot\frac{n}{(n,m)}, v\right)$ Teiler von

$$\lambda\cdot d_1\cdot d_2\cdot\frac{n\cdot m}{(n,m)^2}$$

ist, folgt die Existenz eines solchen μ.

(b) Es sei $n = 2^\alpha\cdot n'$, $m = 2^\beta\cdot m'$, n' und m' ungerade, $\alpha = \beta \geqslant 1$. Zunächst wird der Fall $a > 0$, $b > 0$ betrachtet. Wie im Teil (a) des Beweises geben wir zuerst von $P(a, n) = P(b, m)$ aus und zeigen: Es existieren Zahlen a_1, b_1 aus $\boldsymbol{Z}$ mit

$$a = a_1^{n/d_3}, \quad b = b_1^{m/d_3} \tag{14}$$

und $P(a_1, d_3) = P(b_1, d_3)$. Das Beweisschema ähnelt dem in (a). Anstelle von (7) gilt nach Hilfssatz 9

$$a^{\frac{v}{n}t}\cdot b^{\frac{v}{m}} = d^{\frac{v}{2}} \quad \text{mit} \quad \sqrt{d}\in\boldsymbol{Q}_v. \tag{15}$$

Wie bei (a) ergibt sich

$$[K_f:\boldsymbol{Q}_n] = \frac{(n,m)}{\lambda} \quad \text{mit} \quad \lambda\in\boldsymbol{N}.$$

Nach Hilfssatz 4 besitzt a die Darstellung

$$a = \sqrt[n]{a_2^{2[K_f:\boldsymbol{Q}_n]}} \quad \text{mit} \quad a_2\in\boldsymbol{Z},\ \sqrt{a_2}\in\boldsymbol{Q}_n.$$

Dabei ist der Exponent ganz oder a_2 das Quadrat einer ganzen Zahl. Da eine entsprechende Aussage für b gilt, genügt es zum Nachweis von (14)

$$[K_f:\boldsymbol{Q}_n]\mid d_3, \quad [K_g:\boldsymbol{Q}_m]\mid d_3 \tag{16}$$

zu beweisen. Es sei γ ein Automorphismus des Zerfällungskörpers von $(x^n-a)(x^m-b)$ mit

$$\gamma(\xi_v^{\frac{m}{(n,m)}}) = \xi^{d_3\cdot\lambda\cdot\frac{n\cdot m^2}{(n,m)^3}+\frac{m}{(n,m)}},$$

der den Körper

$$\boldsymbol{Q}_{d_3\cdot\frac{n\cdot m}{(n,m)^2}}$$

invariant läßt. Da

$$[\boldsymbol{Q}_v:\boldsymbol{Q}_{d_3\cdot\frac{n\cdot m}{(n,m)^2}}] \text{ ungerade} \tag{17}$$

ist, bleibt auch $\boldsymbol{Q}(\sqrt[n]{a_2})$ invariant. Hieraus folgt, daß γ so gewählt werden kann, daß außerdem

$$\gamma(\sqrt[n]{a}) = \xi_v^{-d_3\cdot\lambda\cdot\frac{n\cdot m^2}{(n,m)^3}}\cdot\sqrt[n]{a}.$$

Gilt $\gamma(\xi_v)=\xi_v^{1+c}$, so folgt entsprechend (11)

$$c\cdot\frac{m}{(n,m)} \equiv d_3\cdot\lambda\cdot\frac{n\cdot m^2}{(n,m)^3} \pmod v.$$

Wegen (15) und (17) gilt $\gamma(\sqrt[n]{d})=\sqrt[n]{d}$. Der Automorphismus γ läßt die Nullstelle $\xi_n\cdot\sqrt[n]{a}$ von x^n-a fest und damit auch eine Nullstelle von x^m-b, etwa $\xi_m^{\mu}\cdot\sqrt[m]{b}$. Entsprechend (12) erhält man die Kongruenz

$$c\cdot\cdot\frac{n}{(n,m)}\cdot\mu \equiv -t\cdot d_3\cdot\lambda\cdot\frac{n\cdot m^2}{(n,m)^3} \pmod v.$$

Die Auswertung der beiden Kongruenzen liefert $[K_f:\boldsymbol{Q}_n]\,|\,d_3d_2$. Analog läßt sich $[K_g:\boldsymbol{Q}_m]\,|\,d_3d_1$ herleiten. Zusammen mit Hilfssatz 10 folgt insgesamt (16).

Es bleibt $P(a_1,d_3)=P(b_1,d_3)$, oder $P(a,n)=P(a_1,d_3)$ und $P(b,m)=P(b_1,d_3)$ zu beweisen. Nachgewiesen wird die zweite dieser Gleichungen, die dritte folgt dann entsprechend. Nach Hilfssatz 1 genügt es zu zeigen: Ein Automorphismus des Zerfällungskörpers von x^n-a läßt mit einer Nullstelle $\xi_n^{\mu}\cdot\sqrt[n]{a}$ von x^n-a auch eine von $x^{d_3}-a_1$ fest. Wegen (14) besitzt das Bild von $\sqrt[n]{a}$ die Darstellung

$$\xi_n^{\lambda\cdot\frac{n}{d_3}}\cdot\sqrt[n]{a}.$$

Wird ξ_n auf ξ_n^{1+c} abgebildet, so folgt

$$\mu\cdot c \equiv -\lambda\cdot\frac{n}{d_3} \pmod n.$$

Der Automorphismus läßt eine Nullstelle von $x^{d_3}-a_1$ genau dann fest, wenn es ein

$$\mu' \equiv 0\left(\mathrm{mod}\,\frac{n}{d_3}\right)$$

gibt, welches die obige Kongruenz löst. Ein solches μ' existiert jedoch, da

$$\left(\frac{n}{d_3},d_3\right)=1.$$

Es gelte nun umgekehrt (14) und $P(a_1,d_3)=P(b_1,d_3)$. Wie gerade bewiesen wurde, folgt $P(a,n)=P(a_1,d_3)$ und entprechend $P(b,m)=P(b_1,d_3)$, insgesamt also $P(a,n)=P(b,m)$.

Wir betrachten nun den Fall $\alpha=\beta\geqslant 1$ unter der Voraussetzung $ab<0$, also etwa $a<0$, $b>0$. Dann kann es nach Satz 2 aus Vorzeichengründen kein a_1,b_1 aus $\boldsymbol{Z}$ geben derart, daß (14) gilt und $P(a_1,d_3)=P(b_1,d_3)$. Es genügt daher zu zeigen, daß auch $P(a,n)=P(b,m)$ unter diesen Voraussetzungen nicht gelten kann: Es existiert ein Automorphismus von

$$\boldsymbol{Q}_{2v}(\sqrt[n]{|a|},\sqrt[m]{b}),$$

welcher die reellen Wurzeln $\sqrt[n]{|a|},\sqrt[m]{b}$ auf sich abbildet, nicht jedoch i. Dann wird die Nullstelle $\sqrt[m]{b}$ von x^m-b auf sich abgebildet, aber keine Nullstelle von x^n-a, denn diese haben die Form

$$\xi_{2n}^{\mu}\cdot\sqrt[n]{|a|},\quad \mu \text{ ungerade}.$$

Es kann nämlich ξ_{2n}^{μ} nicht auf sich abgebildet werden, weil nach Hilfssatz 7 das Bild von ξ_{2n} die Form ξ_{2n}^{1+c} mit $4\nmid c$ hat.

Es gelte nun $\alpha=\beta\geqslant 1$ und $a<0$, $b<0$. Zunächst wird $P(a,n)=P(b,m)$ angenommen und gezeigt: Es gibt Zahlen a_1,b_1 aus $\boldsymbol{Z}$ derart, daß (14) gilt und $P(a_1,d_3)=P(b_1,d_3)$. Nach Hilfssatz 9 gibt es ein $d\in\boldsymbol{Z}$ derart, daß (15) gilt. Ein Automorphismus von

$$\boldsymbol{Q}_{2v}(\sqrt[n]{|a|},\sqrt[m]{|b|})$$

bildet die reellen Nullstellen $\sqrt[n]{|a|}, \sqrt[m]{|b|}$ auf Elemente der Form $\xi_n^{i'} \cdot \sqrt[n]{|a|}$, $\xi_m^{j'} \cdot \sqrt[m]{|b|}$, und damit wegen (15) sogar auf Elemente der Form

$$\xi_{(n,m)}^{i} \cdot \sqrt[n]{|a|}, \qquad \xi_{(n,m)}^{j} \cdot \sqrt[m]{|b|}$$

ab. Daraus ergibt sich für die Zerfällungskörper K_f, K_g von $x^n - a$, $x^m - b$

$$[(K_f, Q_{2n}) : Q_{2n}] \mid (n, m), \qquad [(K_g, Q_{2m}) : Q_{2m}] \mid (n, m).$$

Darüber hinaus wird gezeigt

$$[(K_f, Q_{2n}) : Q_{2n}] \mid d_3, \qquad [(K_g, Q_{2m}) : Q_{2m}] \mid d_3. \tag{18}$$

Es gelte

$$[(K_f, Q_{2n}) : Q_{2n}] = \frac{(n, m)}{\lambda}.$$

Weiter sei γ ein Automorphismus von $Q_{2v}(\sqrt[n]{|a|}, \sqrt[m]{|b|})$ mit

$$\gamma(\xi_{2v}^{\frac{m}{(n,m)}}) = \xi_{2v}^{2d_3 \cdot \lambda \cdot \frac{n \cdot m^2}{(n,m)^3} + \frac{m}{(n,m)}},$$

der den Körper

$$Q_{2d_3 \cdot \frac{n \cdot m}{(n,m)^2}}$$

invariant läßt. Da Q_{2v} über diesem Körper einen ungeraden Grad besitzt, kann γ ähnlich wie im Fall $a > 0$, $b > 0$ darüber hinaus so gewählt werden, daß

$$\gamma(\sqrt[n]{|a|}) = \xi_{2v}^{-2d_3 \cdot \lambda \cdot \frac{n \cdot m^2}{(n,m)^3}} \cdot \sqrt[n]{|a|}. \tag{19}$$

Die Nullstelle $\xi_{2n} \cdot \sqrt[n]{|a|}$ von $x^n - a$ wird also auf sich abgebildet. Gilt

$$\gamma(\xi_{2v}) = \xi_{2v}^{1+c},$$

so folgt

$$c \cdot \frac{m}{(n, m)} \equiv 2\lambda \cdot d_3 \cdot \frac{n \cdot m^2}{(n, m)^3} \pmod{2v}.$$

Mit einer Nullstelle von $x^n - a$ läßt γ nach Hilfssatz 1 auch eine Nullstelle von $x^m - b$ fest, etwa

$$\xi_{2v}^{\frac{n}{(n,m)} \cdot \mu} \cdot \sqrt[m]{|b|}, \qquad \mu \text{ ungerade}.$$

Wie im Fall $a > 0$, $b > 0$ bildet γ die Zahl $\sqrt{d}$ aus (15) auf sich ab. Wegen (15) und (19) gilt deshalb

$$\gamma(\sqrt[m]{|b|}) = \xi_{2v}^{t 2d_3 \cdot \lambda \cdot \frac{n \cdot m^2}{(n,m)^3}} \cdot \sqrt[m]{|b|}.$$

Zusammen folgt

$$c \cdot \frac{n}{(n, m)} \cdot \mu \equiv -t \cdot d_3 \cdot \lambda \cdot \frac{n \cdot m^2}{(n, m)^3} \pmod{2v}.$$

Eine Auswertung der beiden Kongruenzen liefert

$$[(K_f, Q_{2n}) : Q_{2n}] \mid d_3 d_2.$$

Entsprechend läßt sich

$$[(K_g, Q_{2m}) : Q_{2m}] \mid d_3 d_1$$

herleiten. Zusammen mit Hilfssatz 10 ergibt sich (18).

Für die Zerfällungskörper K_f', K_g' der Polynome $x^n - |a|$, $x^m - |b|$ gilt $[K_f' : Q_n] \mid n$, $[K_g' : Q_m] \mid m$. Zusammen mit (18) folgt daraus $[K_f' : Q_n] \mid d_3$, $[K_g' : Q_m] \mid d_3$, woraus sich (14) ergibt wie im Fall $a > 0$, $b > 0$. Weiter folgt $P(a, n) = P(a_1, d_3)$ und entsprechend $P(b, m) = P(b_1, d_3)$, damit also die zu beweisende Gleichung $P(a_1, d_3) = P(b_1, d_3)$. Dies läßt sich folgendermaßen einsehen. Jede Nullstelle von $x^{d_3} - a_1$ ist auch Nullstelle von $x^n - a$. Ein Automorphismus, der ξ_{2n} auf ξ_{2n}^{1+c} abbildet und $\sqrt[n]{|a|}$ wegen (14) auf ein Element der Form

$$\xi_{2n}^{\lambda \cdot \frac{2n}{d_3}} \cdot \sqrt[n]{|a|},$$

läßt eine Nullstelle von $x^n - a$ fest genau dann, wenn es eine ungerade Zahl μ gibt mit

$$\mu c \equiv -\lambda \cdot \frac{2n}{d_3} \pmod{2n}.$$

Mit μ existiert aber auch eine ungerade Zahl

$$\mu' \equiv 0 \left(\mathrm{mod}\ \frac{n}{d_3}\right),$$

welche die obige Kongruenz löst. Der Automorphismus läßt also mit einer Nullstelle von $x^n - a$ auch eine von $x^{d_3} - a_1$ fest. Gilt nun umgekehrt (14) und $P(a_1, d_3) = P(b_1, d_3)$, so folgt $P(a, n) = P(b, m)$, dies wurde ja gerade mitbewiesen. Damit ist der Fall $\alpha = \beta$ erledigt.

(c) Es sei nun $n = 2^\alpha \cdot n'$, $m = 2^\beta \cdot m'$, n' und m' ungerade und $\alpha < \beta$.

Weiter seien K_f, K_g die Zerfällungskörper von $x^n - a$, $x^m - b$. Zunächst wird der Fall $a < 0, b > 0, a > 0$ betrachtet. Wie im Fall $a \cdot b < 0$, $\alpha = \beta > 0$ kann nicht $P(a, n) = P(b, m)$ gelten, denn ein Automorphismus von (K_f, K_g), welcher die reellen Wurzeln $\sqrt[n]{|a|}$, $\sqrt[m]{b}$, nicht jedoch i auf abbildet, läßt die Nullstelle $\sqrt[m]{b}$ von $x^m - b$, aber keine Nullstelle von $x^n - a$ fest. Entsprechend folgt aus $a > 0$, $b < 0$, $a > 0$, daß $P(a, n) \neq P(b, m)$ ist. Im Fall $a = 0$ gilt offenbar $P(a, n) = P(a^2, 2n)$.

Wir betrachten nun den Fall $a > 0$, $b > 0$, $1 \leqq \alpha < \beta$. Es sei zunächst $P(a, n) = P(b, m)$. Nach Hilssatz 9 gibt es natürliche Zahlen $t, d, 0 < t < v$, $(t, v) = 1$ mit

$$a^{\frac{v}{n}t} \cdot b^{\frac{v}{m}} = d^{\frac{v}{2}}, \qquad \sqrt{d} \in \boldsymbol{Q}_v. \tag{20}$$

Wie in den Fällen (a) und (b) folgt, daß $[K_f : \boldsymbol{Q}_n]$ und $[K_g : \boldsymbol{Q}_m]$ Teiler von (n, m) sind. Es gelte

$$[K_f : \boldsymbol{Q}_n] = \frac{(n, m)}{\lambda_1}.$$

Nach Hilfssatz 4 besitzt a die Darstellung

$$a = a_2^{\frac{n}{2[K_f : \boldsymbol{Q}_n]}} \quad \text{mit} \quad a_2 \in \boldsymbol{Z}, \sqrt{a_2} \in \boldsymbol{Q}_n.$$

Es sei γ_1 ein Automorphismus von (K_f, K_g) mit

$$\gamma_1(\xi_v^{\frac{m}{(n,m)}}) = \xi_v^{2^\alpha d_3 \cdot \lambda_1 \cdot \frac{n \cdot m^2}{(n,m)^3} + \frac{m}{(n,m)}},$$

der den Körper

$$\boldsymbol{Q}_{2^\alpha d_3 \cdot \frac{n \cdot m}{(n,m)^2}}$$

invariant läßt. Da $\boldsymbol{Q}_v$ über diesem Körper einen ungeraden Grad besitzt, wird $\sqrt{a_2}$ auf sich abgebildet. Hieraus folgt, daß γ_1 so gewählt werden kann, daß

$$\gamma_1(\sqrt[n]{a}) = \xi_v^{-2^\alpha d_3 \cdot \lambda_1 \cdot \frac{n \cdot m^2}{(n,m)^3}} \cdot \sqrt[n]{a}.$$

Gilt $\gamma_1(\xi_v) = \xi_v^{1+c}$, so folgt

$$c \cdot \frac{m}{(n, m)} \equiv 2^\alpha \lambda_1 \cdot d_3 \cdot \frac{n \cdot m^2}{(n, m)^3} \pmod{v}.$$

Mit der Nullstelle $\xi_n \cdot \sqrt[n]{a}$ von $x^n - a$ läßt γ_1 auch eine Nullstelle von $x^m - b$

fest, etwa $\xi_m^\mu \cdot \sqrt[m]{b}$. Da ebenso wie $\sqrt{a_2}$ auch $\sqrt{d}$ auf sich abgebildet wird, folgt nach (20)

$$c \cdot \frac{n}{(n, m)} \cdot \mu \equiv -t \cdot 2^\alpha \cdot \lambda_1 \cdot d_3 \cdot \frac{n \cdot m^2}{(n, m)^3} \pmod{v}.$$

Aus den beiden Kongruenzen ergibt sich $d_1 \mid \lambda_1$, also

$$[K_f : \boldsymbol{Q}_n] \mid d_3 \cdot d_2. \tag{21}$$

Wir beweisen nun

$$[K_g : \boldsymbol{Q}_m] \mid d_3 \cdot d_1. \tag{22}$$

Die vorangegangenen Betrachtungen lassen sich hier nicht ohne weiteres übertragen, da $\alpha \neq \beta$ ist. Es gelte

$$[K_g : \boldsymbol{Q}_m] = \frac{(n, m)}{\lambda_2}.$$

Dann hat b die Darstellung

$$b = b_2^{\frac{m}{2[K_g : \boldsymbol{Q}_m]}} \quad \text{mit} \quad b_2 \in \boldsymbol{Z}, \sqrt{b_2} \in \boldsymbol{Q}_m.$$

Wir nehmen zunächst an, daß es einen Automorphismus γ_2 von (K_f, K_g) gibt mit

$$\gamma_2(\xi_v^{\frac{n}{(n,m)}}) = \xi_v^{d_3 \cdot \lambda_2 \cdot \frac{n^2 \cdot m}{(n,m)^3} + \frac{n}{(n,m)}}, \tag{23}$$

der den Körper

$$\boldsymbol{Q}_r = \boldsymbol{Q}_{\left(d_3 \cdot \lambda_2 \cdot \frac{n \cdot m}{(n,m)^2}, v\right)} \quad \text{invariant} \tag{24}$$

läßt und $\sqrt{b_2}$, $\sqrt{d}$ auf sich abbildet. Wir werden gleich sehen, daß ein solcher Automorphismus immer existiert. Dann kann γ_2 so gewählt werden, daß

$$\gamma_2(\sqrt[m]{b}) = \xi_v^{-d_3 \cdot \lambda_2 \cdot \frac{n^2 \cdot m}{(n,m)^3}} \cdot \sqrt[m]{b}.$$

Gilt

$$\gamma_2(\xi_v) = \xi_v^{1+c_1},$$

so folgt

$$c_1 \cdot \frac{n}{(n, m)} \equiv \lambda_2 \cdot d_3 \cdot \frac{n^2 \cdot m}{(n, m)^3} \pmod{v}.$$

Mit der Nullstelle $\xi_m \cdot \sqrt[m]{b}$ von $x^m - b$ läßt γ_2 auch eine Nullstelle von $x^n - a$

fest, etwa $\xi_n^{\mu} \cdot \sqrt[n]{a}$. Aus (20) folgt

$$c_1 \cdot \frac{m}{(n,m)} \cdot \mu \cdot t \equiv -\lambda_2 \cdot d_3 \cdot \frac{n^2 \cdot m}{(n,m)^3} \pmod{v}.$$

Die Auswertung der beiden Kongruenzen liefert (22).

Zum Beweis von (22) muß noch die Existenz eines Automorphismus γ_2 mit den oben genannten Eigenschaften nachgewiesen werden. Im Fall

$$8 \mid \lambda_2 \cdot \frac{m}{(n,m)} \quad \text{oder} \quad 2^{\alpha} \mid \lambda_2$$

ist dies trivial, da dann nach Hilfssatz 5 der Körper $\boldsymbol{Q}_r$ genau dieselben quadratischen Teilkörper wie $\boldsymbol{Q}_v$ enthält, also auch $\sqrt{b_2}$ und $\sqrt{d}$. Existiert kein Automorphismus mit den Eigenschaften (23) und (24), welcher $\sqrt{b_2}, \sqrt{d}$ auf sich abbildet, so gibt es einen Automorphismus γ_3 mit

$$\gamma_3(\xi_v^{\frac{n}{(n,m)}}) = \xi_v^{2d_3 \cdot \lambda_2 \cdot \frac{n^2 \cdot m}{(n,m)^3} + \frac{n}{(n,m)}},$$

welcher

$$\boldsymbol{Q}_{2r} \text{ invariant}$$

läßt und $\sqrt{b_2}, \sqrt{d}$ auf sich abbildet. Dann lassen sich die beiden obigen Kongruenzen entsprechend herleiten mit der Einschränkung, daß auf den rechten Seiten der Faktor 2 hinzugefügt werden muß. Eine Auswertung dieser beiden Kongruenzen liefert $\frac{d_2}{2} \mid \lambda_2$ und damit

$$2^{\beta-1} \mid \lambda_2 \cdot \frac{m}{(n,m)}.$$

Nach dem zu Anfang erledigtem Fall ist die Existenz von γ_2 für $\beta > 3$ damit nachgewiesen. Ebenfalls folgt (22) nach Definition von λ_2, falls $[K_g : \boldsymbol{Q}_m]$ ungerade ist. Außerdem ergibt sich nach Hilfssatz 5, daß jeder quadratische Teilkörper von $\boldsymbol{Q}_n$, also auch $\sqrt{a_2}$, in $\boldsymbol{Q}_r$ enthalten ist. Die Zahl $\sqrt{a_2}$ bleibt also bei Anwendung eines Automorphismus mit den Eigenschaften (23) und (24) fest, wegen (20) werden dann $\sqrt{b_2}, \sqrt{d}$ entweder beide auf sich oder beide nicht auf sich abgebildet. Wir sind also sicher fertig, falls

$$\boldsymbol{Q}_r(\sqrt{b_2}) \neq \boldsymbol{Q}_{2r}$$

ist. Anderenfalls kann ein Automorphismus mit den Eigenschaften (23) und (24) die Zahl $\sqrt{b_2}$ nicht auf sich abbilden, also auch keine Nullstelle

von $x^m - b$, da das Bild der $\frac{(n,m)}{\lambda_2}$-ten Potenz einer Nullstelle offenbar durch Multiplikation mit -1 entsteht. Ist

$$\boldsymbol{Q}_{2r} \nsubseteq \boldsymbol{Q}_r(\sqrt[n]{a}),$$

so gibt es andererseits einen Automorphismus mit den Eigenschaften (23) und (24), welcher die Nullstelle $\sqrt[n]{a}$ von $x^n - a$ auf sich abbildet. Die letzte Beziehung ist sicher erfüllt, falls $[K_f : \boldsymbol{Q}_n]$ ungerade ist. In diesem Fall sind wir also fertig. Es sei nun $[K_f : \boldsymbol{Q}_n] \equiv 2 \pmod 4$. Wie bereits festgestellt wurde kann

$$[K_g : \boldsymbol{Q}_m] \text{ gerade, also } \sqrt[4]{b_2} \notin \boldsymbol{Q}_v$$

und

$$\sqrt[n]{a}^{\frac{[K_f:\boldsymbol{Q}_n]}{2}} \in \boldsymbol{Q}_{2r}, \quad \text{also} \quad [K_f : \boldsymbol{Q}_v] \text{ ungerade}$$

angenommen werden. Dann gibt es einen Automorphismus, der $\boldsymbol{Q}_v$ invariant läßt, die Nullstelle $\sqrt[n]{a}$ von $x^n - a$ auf sich abbildet, nicht jedoch $\sqrt[4]{b_2}$ und damit auch nicht $\sqrt[m]{b}$, also keine Nullstelle von $x^m - b$. Da wir uns nach den bisherigen Betrachtungen auf $\beta \leqslant 3$, also $\alpha \leqslant 2$ beschränken können, bleibt nur noch der Fall $[K_f : \boldsymbol{Q}_n] \equiv 0 \pmod 4$ zu betrachten. Dann gibt es einen Automorphismus, der $\sqrt[n]{a}$ auf $i \cdot \sqrt[n]{a}$ abbildet und keinen von $\boldsymbol{Q}$ verschiedenen Kreisteilungskörper invariant läßt. Nach Hilfssatz 7 läßt dieser Automorphismus keine Nullstelle von $x^n - a$ fest, nach (20) jedoch eine von $x^m - b$. Dies ist ein Widerspruch zu $P(a,n) = P(b,m)$. Damit ist (22) bewiesen.

Da sich die Körpergrade $[K_f : \boldsymbol{Q}_n]$ und $[K_g : \boldsymbol{Q}_m]$ nach Hilfssatz 10 höchstens um den Faktor 2 unterscheiden, ergibt sich aus (21) und (22)

$$[K_g : \boldsymbol{Q}_m] \mid d_3, \quad [K_f : \boldsymbol{Q}_n] \mid 2d_3.$$

Nach Hilfssatz 4 gibt es ein $b_1 \in \boldsymbol{N}$ mit

$$b = b_1^{m/2d_3}. \tag{25}$$

Entsprechend gibt es ein $a_1 \in \boldsymbol{N}$ mit

$$a = a_1^{n/2d_3}. \tag{26}$$

Dies ist klar, falls $[K_f : \boldsymbol{Q}_n] \mid d_3$ ist. Anderenfalls gilt nach Hilfssatz 10

$$[K_f : \boldsymbol{Q}_n] = 2[K_g : \boldsymbol{Q}_m].$$

Da K_f über Q_n zyklisch ist, gibt es genau einen Teilkörper von K_f vom Grad 2 über Q_n, nämlich

$$Q_n(\sqrt[n]{a}^{\frac{[K_f:Q_n]}{2}}).$$

Dem Beweis von Hilfssatz 10 ist zu entnehmen, daß dieser in Q_m enthalten sein muß. Nach Hilfssatz 4 gibt es ein $a_2 \in N$ mit

$$a = a_2 \sqrt[n]{2[K_f:Q_n]}.$$

Dann ist

$$\sqrt[n]{a}^{\frac{[K_f:Q_n]}{2}} = a_2^{1/4} \in Q_m.$$

Daraus folgt nach Hilfssatz 4, daß a_2 das Quadrat einer natürlichen Zahl ist. Damit ist (26) bewiesen. Die weiteren Betrachtungen werden nun in verschiedene Fälle aufgeteilt. Benutzt werden dabei die Beziehungen (20), (25), (26).

Sind a_1 und b_1 Quadratzahlen, so ist die Zahl d aus (20) das Quadrat einer ganzen Zahl. Ein Automorphismus γ des Zerfällungskörpers von $(x^n-a)(x^m-b)$ bildet dann $\sqrt[n]{a}$ auf ein Element der Form

$$\xi_v^{-\lambda \cdot d_1 \cdot d_2 \cdot \frac{n \cdot m}{(n,m)^2}} \cdot \sqrt[n]{a}$$

ab. Gilt $\gamma(\xi_v) = \xi_v^{1+c}$, so bleibt eine Nullstelle von x^n-a fest genau dann, wenn es ein δ gibt mit

$$\delta \cdot c \cdot \frac{m}{(n,m)} \equiv \lambda \cdot d_1 \cdot d_2 \cdot \frac{n \cdot m}{(n,m)^2} \pmod{v}, \tag{27}$$

und eine Nullstelle von x^m-b nach (20) genau dann, wenn es ein μ gibt mit

$$\mu \cdot c \cdot \frac{n}{(n,m)} \equiv -t \cdot \lambda \cdot d_1 \cdot d_2 \cdot \frac{n \cdot m}{(n,m)^2} \pmod{v}.$$

Beides ist gleichwertig, nämlich genau dann der Fall, wenn $(c, d_3) \mid \lambda$ ist.

Ist a_1 Quadratzahl, nicht jedoch b_1, so ist die Zahl d aus (20) nicht das Quadrat einer ganzen Zahl. Wir übernehmen die Bezeichnungen vom obigen Fall. Dann läßt γ eine Nullstelle von x^n-a wieder genau dann fest, wenn es ein δ mit der Eigenschaft (27) gibt, und eine Nullstelle von

x^m-b nach (20) genau dann, wenn es ein μ gibt mit

$$\mu \cdot c \cdot \frac{n}{(n,m)} \equiv -t \cdot \lambda \cdot d_1 \cdot d_2 \cdot \frac{n \cdot m}{(n,m)^2} \pmod{v}$$

bzw.

$$\mu \cdot c \cdot \frac{n}{(n,m)} \equiv -t \cdot \lambda \cdot d_1 \cdot d_2 \cdot \frac{n \cdot m}{(n,m)^2} + \frac{v}{2} \pmod{v},$$

je nach dem ob $\sqrt{d}$ durch γ auf sich abgebildet wird oder nicht. Mit μ existiert immer auch ein δ mit der entsprechenden Kongruenzeigenschaft. Umgekehrt gibt es mit δ auch ein μ genau dann, wenn es keinen Automorphismus γ gibt mit $2^\beta \mid c$, der eine Nullstelle von x^n-a auf sich abbildet, nicht jedoch $\sqrt{d}$. Die Bedingung $2^\beta \mid c$ ist gleichwertig damit, daß γ den Körper Q_{2^β} invariant läßt. Da a_1 nach Annahme Quadratzahl ist, muß nach Hilfssatz 11

$$[Q(\sqrt[2d_3]{a_1}) : Q]$$

und damit auch

$$[Q_{2^\beta}(\sqrt[2d_3]{a_1}) : Q_{2^\beta}]$$

ungerade sein. Der Körper

$$Q_{2^\beta}(\sqrt[2d_3]{a_1})$$

enthält also nach Hilfssatz 5 höchstens einen reellen quadratischen Zahlkörper, und zwar den Körper $Q(\sqrt{2})$ genau dann, wenn $\beta \geqslant 3$ ist, andererseits enthält er jedoch die Nullstelle $\sqrt[n]{a}$ von x^n-a. Hieraus folgt, daß mit δ auch ein μ existiert genau dann, wenn $Q(\sqrt{d}) = Q(\sqrt{2})$ und $\beta \geqslant 3$ ist. Nach Hilfssatz 1 liefert dies die Behauptung von Satz 4 für den betrachteten Fall.

Wir nehmen nun an, daß a_1 nicht Quadratzahl ist. Ein Automorphismus bildet dann $\sqrt[n]{a}$ auf ein Element der Form

$$\xi_v^{-\lambda \cdot d_1 \cdot d_2 \cdot \frac{n \cdot m}{(n,m)^2} \cdot \frac{1}{2}} \cdot \sqrt[n]{a}$$

ab. Dabei ist λ gerade genau dann, wenn $\sqrt{a_1}$ auf sich abgebildet wird. Ist das Bild von ξ_v wieder ξ_v^{1+c}, so bleibt eine Nullstelle von x^n-a genau dann fest, wenn es ein δ gibt mit

$$\delta \cdot c \cdot \frac{m}{(n,m)} \equiv \lambda \cdot d_1 \cdot d_2 \cdot \frac{n \cdot m}{(n,m)^2} \cdot \frac{1}{2} \pmod{v},$$

und eine Nullstelle von $x^m - b$ genau dann, wenn es ein μ gibt mit

$$\mu \cdot c \cdot \frac{n}{(n,m)} \equiv -t \cdot \lambda \cdot d_1 \cdot d_2 \cdot \frac{n \cdot m}{(n,m)^2} \cdot \frac{1}{2} \pmod{v}$$

bzw.

$$\mu \cdot c \cdot \frac{n}{(n,m)} \equiv -t \cdot \lambda \cdot d_1 \cdot d_2 \cdot \frac{n \cdot m}{(n,m)^2} \cdot \frac{1}{2} + \frac{v}{2} \pmod{v},$$

je nach dem ob $\sqrt{d}$ auf sich abgebildet wird oder nicht. Es existiert ein μ, aber kein δ genau dann, wenn $2^\alpha \| c$, λ ungerade ist, und eine Nullstelle von $x^m - b$ fest bleibt. Einen Automorphismus mit diesen Eigenschaften gibt es genau dann nicht, wenn $Q(\sqrt{a_1}) \subseteq Q_{2^\alpha}$, nach Hilfssatz 5 also $\alpha \geqslant 3$ und $Q(\sqrt{a_1}) = Q(\sqrt{2})$ ist. Dies läßt sich folgendermaßen einsehen. Ist $Q(\sqrt{a_1}) \nsubseteq Q_{2^\alpha}$, so gibt es einen Automorphismus, der den Körper

$$Q_{2^\alpha}(\overset{d_3}{\sqrt{a_1}})$$

invariant läßt, nicht jedoch $Q(\sqrt{a_1})$, Q_{2^β}, denn nach Hilfssatz 11 ist

$$[Q_{2^\alpha}(\overset{d_3}{\sqrt{a_1}}) : Q_{2^\alpha}]$$

ungerade. Für diesen Automorphismus gilt $2^\alpha \| c$, $\lambda = d_3$ ungerade. Da $2^\beta \nmid c$ und wegen (20) die Zahl $\overset{m}{\sqrt{b}}$ auf $\overset{m}{\sqrt{b}}$ oder $-\overset{m}{\sqrt{b}}$ abgebildet wird, bleibt nach Hilfssatz 8 außerdem eine Nullstelle von $x^m - b$ fest.

Es existiert ein δ, aber kein μ genau dann, wenn $2^\beta \| c$, λ gerade ist, $\sqrt{d}$ auf $-\sqrt{d}$ abgebildet wird und eine Nullstelle von $x^n - a$ auf sich abgebildet wird. Einen Automorphismus mit diesen Eigenschaften gibt es genau dann nicht, wenn $Q(\sqrt{d}) \subseteq Q_{2^\beta}(\sqrt{a_1})$, denn $Q_{2^\beta}(\overset{n}{\sqrt{a}})$ enthält eine Nullstelle von $x^n - a$, aber nicht mehr quadratische Teilkörper als $Q_{2^\beta}(\overset{2}{\sqrt{a_1}})$. Insgesamt ergibt sich, daß $P(a,n) = P(b,n)$ in diesem Fall gleichwertig ist mit $\alpha \geqslant 3$, $Q(\sqrt{d}) \subseteq Q(\sqrt{a_1}) = Q(\sqrt{2})$.

Es bleibt der Fall $1 \leqslant \alpha < \beta$, $a < 0$, $b < 0$ zu untersuchen. Aus $\beta > 2$ folgt nach Hilfssatz 9 durch Vorzeichenüberlegungen $P(a,n) \neq P(b,m)$. Wir können also von $\alpha = 1$, $\beta = 2$ ausgehen. Es gelte zunächst $P(a,n) = P(b,m)$. Vorzeichenbetrachtungen liefern nach Hilfssatz 9, daß es ganze Zahlen t, d mit $0 < t < v$, $(t,v) = 1$ gibt derart, daß

$$a^{\frac{v}{n}t} \cdot b^{\frac{v}{m}} = -2^{\frac{v}{2}} d^{\frac{v}{2}}, \qquad \sqrt{d} \in Q_v.$$

Hieraus ergibt sich sofort, daß

$$|b|^{v/m}$$

und damit auch $|b|$ Quadrat einer Zahl aus $\boldsymbol{Z}$ ist. Wir zeigen darüber hinaus, daß dies auch für $|a|$ gilt. Zum indirekten Beweis wird angenommen, daß $|a|$ nicht Quadratzahl ist. Dann gibt es nach Hilfss tz 11 einen Automorphismus γ_1 von (K_f, Q_{2n}) mit

$$\gamma_1(i) = -i, \qquad \gamma_1(\sqrt{|a|}) = -\sqrt{|a|}, \qquad \gamma_1(\overset{n/2}{\sqrt{|a|}}) = \overset{n/2}{\sqrt{|a|}}.$$

Die Nullstelle $i \cdot \overset{n}{\sqrt{|a|}}$ von $x^n - a$ wird also auf sich abgebildet. Nach Hilfssatz 1 ergibt sich hieraus ein Widerspruch, da ein Automorphismus γ_2 von (K_g, Q_{2m}) mit $\gamma_2(i) = -i$ keine Nullstelle

$$\xi_{2m}^{j_1} \cdot \overset{m}{\sqrt{|b|}}, \qquad j_1 \equiv 1 \pmod 2$$

von $x^m - b$ auf sich abbilden kann. Dies ergibt sich folgendermaßen: Ist

$$\gamma_2(\xi_{2m}) = \xi_{2m}^{1+c},$$

so gilt nach Hilfssatz 7 die Kongruenz

$$c \equiv 2 \pmod 4.$$

Da $|b|$ Quadratzahl ist, hat das Bild von $\overset{m}{\sqrt{|b|}}$ andererseits die Form

$$\gamma_2(\overset{m}{\sqrt{|b|}}) = \xi_{2m}^{4j_2} \cdot \overset{m}{\sqrt{|b|}}.$$

Es genügt nun zu zeigen: Wenn $|a|$ Quadrat einer Zahl aus $\boldsymbol{Z}$ ist, $a < 0$, $n \equiv 2 \pmod 4$, so gilt

$$P(a,n) = P(-2^n a^2, 2n).$$

Es sei γ_3 ein Automorphismus von

$$Q_{4n}(\overset{n}{\sqrt{|a|}})$$

mit

$$\gamma_3(\xi_{4n}) = \xi_{4n}^{1+c}.$$

Da $|a|$ Quadratzahl ist, hat das Bild von $\overset{n}{\sqrt{|a|}}$ die Form

$$\gamma_3(\overset{n}{\sqrt{|a|}}) = \xi_{4n}^{8j_3} \cdot \overset{n}{\sqrt{|a|}}.$$

Die Nullstellen von $x^n - a$ bzw. $x^{2n} + 2^n a^2$ sind

$$\xi_{4n}^{j_4} \cdot \overset{n}{\sqrt{|a|}}, \qquad j_4 \equiv 2 \pmod 4,$$

bzw.

$$\xi_{4n}^{j_5} \cdot \overset{n}{\sqrt{|a|}}\sqrt{2}, \qquad j_5 \equiv 1 \pmod 2.$$

Ist $c \equiv 2 \pmod 4$, so läßt γ_3 offenbar keine Nullstelle von $x^n - a$ oder $x^{2n} + 2^n a^2$ fest. Ist $c \equiv 0 \pmod 8$, so gilt $\gamma_3(\sqrt{2}) = \sqrt{2}$, und γ_3 läßt eine Nullstelle von $x^n - a$ bzw. $x^{2n} + 2^n a^2$ genau dann fest, wenn es ein $j_4 \equiv 2 \pmod 4$ gibt mit

$$c \cdot j_4 \equiv -8j_3 \pmod{4n},$$

bzw. ein $j_5 \equiv 1 \pmod 2$ mit

$$c \cdot j_5 \equiv -8j_3 \pmod{4n}.$$

Beides ist genau dann der Fall, wenn $(c, 4n) \mid 8j_3$. Ist $c \equiv 4 \pmod 8$ so gilt $\gamma_3(\sqrt{2}) = -\sqrt{2}$. Dann läßt γ_3 eine Nullstelle von $x^n - a$ fest genau dann, wenn es ein $j_4 \equiv 2 \pmod 4$ gibt mit

$$cj_4 \equiv -8j_3 \pmod{4n},$$

also genau dann, wenn

$$(c, 4n) \mid 8j_3.$$

Eine Nullstelle von $x^{2n} + 2^n a^2$ bleibt genau dann fest, wenn es ein $j_5 \equiv 1 \pmod 2$ gibt mit

$$cj_5 \equiv -8j_3 + 2n \pmod{4n},$$

also genau dann, wenn

$$(c, 4n) \nmid (-8j_3 + 2n).$$

Beide Teilerbedingungen sind gleichwertig. Nach Hilfssatz 1 ergibt sich also die Behauptung. Damit ist Satz 4 bewiesen.

Literaturverzeichnis

[1] N. C. Ankeny and C. A. Rogers, *A conjecture of Chowla*, Ann. of Math. 53 (1951), S. 541–550.

[2] H. Flanders, *Generalisation of a theorem of Ankeny and Rogers*, ibid. 57 (1953), S. 392–400.

[3] I. Gerst, *On the theory of n-th power residues and a conjecture of Kronecker*, Acta Arith. 17 (1970), S. 121–139.

[4] A. Schinzel, *A refinement of a theorem of Gerst on power residues*, ibid. 17 (1970), S. 161–168.

[5] V. Schulze, *Die Verteilung der Primteiler von Polynomen auf Restklassen II*, Journ. Reine Angew. Math. 281 (1976), S. 126–148.

[6] E. Trost, *Zur Theorie der Potenzreste*, Nieuw Arch. Wiskunde 18 (1934), S. 58–61.

Eingegangen am 13. 2. 1976
und in revidierter Form am 14. 5. 1976 (815)

ACTA ARITHMETICA
XXXIII (1977)

An explicit bound for Iwasawa's λ-invariant

by

BRUCE FERRERO (Cambridge, Mass.)

For each finite extension k of the field $\boldsymbol{Q}$ of rational numbers, and for each prime number p, Iwasawa has defined a non-negative integer $\lambda_p(k)$ (see [4] for a description of the meaning of this invariant). We will give an explicit bound for $\lambda_p(k)$, for all p, when k is one of the ten imaginary quadratic fields described below. The method used is a refinement of a technique of Metsänkylä [5].

THEOREM. *Let $k = \boldsymbol{Q}(\sqrt{-d})$ be the imaginary quadratic field of discriminant $-d$, where $d \leqslant 20$, $d = 24$, or $d = 40$. Then for each prime number p, we have $\lambda_p(k) < p^{3(p-1)/2}$.*

Proof. If $p \leqslant 7$ and $p \leqslant d$, if $p = d = 11$, or if $p = d = 19$, then the validity of the theorem may be checked by calculating the exact value of $\lambda_p(k)$ (usually 0 or 1) by the formulas of [2]. We will therefore assume that $p \nmid d$ and that p is greater than the minimum of d and 7.

Let $\boldsymbol{Z}_p$ and $\boldsymbol{Q}_p$ denote respectively the ring of p-adic integers and field of p-adic numbers. Let χ be the Dirichlet character for k; then χ has conductor d, is defined on the rational integers $\boldsymbol{Z}$, and assumes the values -1, 0, and 1. Let $\omega: \boldsymbol{Z} \to \boldsymbol{Z}_p$ be the Dirichlet character of conductor p which satisfies the congruence $\omega(a) \equiv a \pmod p$, for all $a \in \boldsymbol{Z}$. Let $L_p(s; \chi\omega)$ be the p-adic L-function for the character $\chi\omega$ (see [3] for the definition). Then $L_p(s; \chi\omega)$ is defined for $s \in \boldsymbol{Z}_p$ and takes values in $\boldsymbol{Z}_p$ for such s. The main step in the proof consists in showing that if n is a nonnegative integer such that $\lambda_p(k) \geqslant p^n$, then $L_p(s; \chi\omega)$ is divisible by p^{n+1}, for all $s \in \boldsymbol{Z}_p$.

Let w be the number of roots of 1 in k. Define, for any $b, c \in \boldsymbol{Z}$, a rational number $h(b, c)$ by

$$h(b, c) = (-w/2d) \sum_{j=1}^{d-1} j\chi(b + cj).$$

Then the following properties are easily verified:

(i) $h(b, c) = \chi(c)h(b', 1)$, if $b' \in \boldsymbol{Z}$ and $b \equiv b'c \pmod d$;